Some Dilemmas Regarding Payment Card Related Crimes

VARSTVOSLOVJE, Journal of Criminal Justice and Security year 14 no. 2 pp. 191-204

Igor Lamberger, Bojan Dobovšek, Boštjan Slak

Purpose:

The number of crimes which involve payment cards is increasing, and there are numerous types of misuse, abuse and fraud. However, there is a substantial lack of criminal literature and information about how to investigate and prevent these types of crimes. This article is an attempt to provide concise basic information regarding these crimes. But we have to remain cautious as whoever undertakes the task of presenting criminal investigative methods (of actually any type of crime) risks giving away knowledge and information to criminals. This should especially be considered when dealing with crimes related to payment cards.

Design/Methods/Approach:

This article is based on reviews of expert literature and experiences derived from practical cases. The approach is positivistic; theoretically the paper is about crimes related to payment cards.

Findings:

Literature dedicated to criminal investigation aspects of payment card related crimes is rare. There are, however, numerous publications on the technological scope of these crimes, including manuals about preventive measures (e.g. computer networks, mathematical protection algorithms), yet it seems that perpetrators are a step ahead as the number of payment card related crimes is not decreasing. Prevention is still the best action.

Research Limitations/Implications:

In-depth case studies can't be done easily because information about the perpetrators who were apprehended is classified, and banks are also not willing to share information about security system breaches or attacks on ATMs.

Practical Implications:

Showing some characteristics of payment card fraud could be useful to investigators. It is also good to disprove some myths about these types of crimes, and to emphasize the importance of institutional cooperation. It could bring about some progress in developing more expert networks.

Originality/Value:

Literature on the subject of payment card crimes is rare. Especially rare are presentations of this problem from the criminal investigation aspect, so this article brings some practical insights and concise information about crimes related to payment cards, and the accompanying professional dilemmas.

UDC: 343.3/.7

Keywords: payment cards, credit cards, frauds, counterfeit credit cards, investigation, prevention

Nekatere dileme glede kaznivih dejanj, povezanih s plačilnimi karticami

Namen:

Število kaznivih dejanj, povezanih s plačilnimi karticami, se povečuje. Obstajajo številne pod-vrste zlorab in goljufij. Opazno je veliko pomanjkanje literature in kriminalističnih informacij o načinu preiskovanja in tudi preprečevanja tovrstnih kaznivih dejanj. Namen članka je zatorej povzeti nekaj osnovnih informacij o tovrstnih kaznivih dejanjih. Pri tem pa moramo biti previdni, saj kdor koli prevzame nalogo, da predstavi kriminalistične metode za preiskovanje teh kaznivih dejanj (pravzaprav vseh vrst), tvega širjenje znanja in ozaveščanje storilcev. In kazniva dejanja, povezana s plačilnimi karticami, so vrsta kaznivih dejanj, pri katerih je treba to upoštevati še bolj dosledno.

Metode:

Pregled literature in spoznanj iz prakse. S pozitivističnim pristopom smo analizirali problematiko kaznivih dejanj v zvezi s plačilnimi karticami.

Ugotovitve:

Kriminalistične literature o kaznivih dejanjih s plačilnimi karticami je malo, obstajajo pa številne objave na tehnološkem (preventivnem) področju zoper te vrste kaznivih dejanj (računalniška omrežja, matematični algoritmi za zaščito). Vendar se zdi, da storilci kaznivih dejanj ostajajo korak pred njimi, saj se število kaznivih dejanj, povezanih s plačilnimi karticami, ne zmanjšuje. Preventiva je še vedno najboljši ukrep.

Omejitve/uporabnost raziskave:

Poglobljenih študij primerov ni mogoče narediti zaradi varovanih podatkov odkritih storilcev, poleg tega pa tudi banke ne dajejo informacij o vdorih v njihove varnostne sisteme ali bankomate.

Praktična uporabnost:

Za preiskovalce bodo koristne nekatere prikazane značilnosti kaznivih dejanj, povezanih s plačilnimi karticami. Uporabnost vidimo tudi v odpravi nekaterih mitov o tej vrsti kaznivih dejanj. Poudarjanje pomembnosti sodelovanja institucij, kar prinaša določen napredek, bi lahko botrovalo razvoju več takšnih delovnih omrežij.

Izvirnost/pomembnost prispevka:

Literatura na temo kaznivih dejanj s plačilnimi karticami je redka. Predvsem iz področja preiskovanja, tako da članek prinaša nekaj praktičnih vpogledov v problematiko in nekaj strnjenih informacij ter dilem v zvezi s tovrstno kriminaliteto.

UDK: 343.3/.7

Ključne besede: plačilne kartice, kreditne kartice, goljufije, ponarejanje kartic, preiskovanje, preventiva

1 INTRODUCTION – PAYMENT CARD FRAUDS

Payment cards[1] are constructed in the form of standardized plastic cards with embossed records, data on the magnetic (data) stripe, and/or data records in an electronic circuit (the chip). In all three cases the card contains some information about the cardholder, e.g. the issuing bank and payment options. This reference data, stored on the magnetic stripe and/or chip, is compared to data in a central database before a transaction is executed (Lamberger, 2011). And with every payment method, no matter how widespread it is, there are accompanying frauds. In this regard, payment cards are no exception, even though it is claimed that they come with the best security measures possible. Classical types of payment card fraud (skimming) accumulated more than 350 million Euros worth of damages in the EU region alone in 2009 (EUROPOL Review, 2011), while the total accumulated damage of credit card abuse (all types included) the damage in the EU was over 1.5 billion Euros (EUROPOL, 2011).

Among the possible security measures, the most prevailing is the so called PCI standard, which is a product of the commitment of the five largest issuers of payment cards (VISA, MasterCard, American Express, Discover Financial Services, and JCB International), intended to ensure that the use of payment cards is safer and more systematized. It is a collection of mandatory recommendations that are required to be implemented by all those who wish to use card services. These recommendations include mandatory instructions for legal entities (merchants and service providers, card issuer, etc.) for establishing the appropriate information systems, providing system management and implementing security policies to protect data and information related to payments or issued cards (Pcistandard.com, 2011; PCI Security Standards Council, 2011). Despite the fact that the standard is a collection of good and effective measures, the trend in payment card abuse has not significantly fallen, given that the PCI standard dates back to 2004. The trend in the number of abuses did not significantly slow down even after the introduction of chips for storing relevant data (so improving the safety of stored data) on the payment card (Prabowo, 2011). A major reason for this safety drawback is the fact that the methods *chip + PIN* or *chip + signature authorization* were not adopted globally. The following figure shows the degree of EMV standard implementation.

1 *We use the term "payment cards" instead of the more commonly used term "credit cards", due to the fact that credit cards are only one sub-type of payment cards, which are consisted from several different types, and all those types can be abused or misused in some way.*

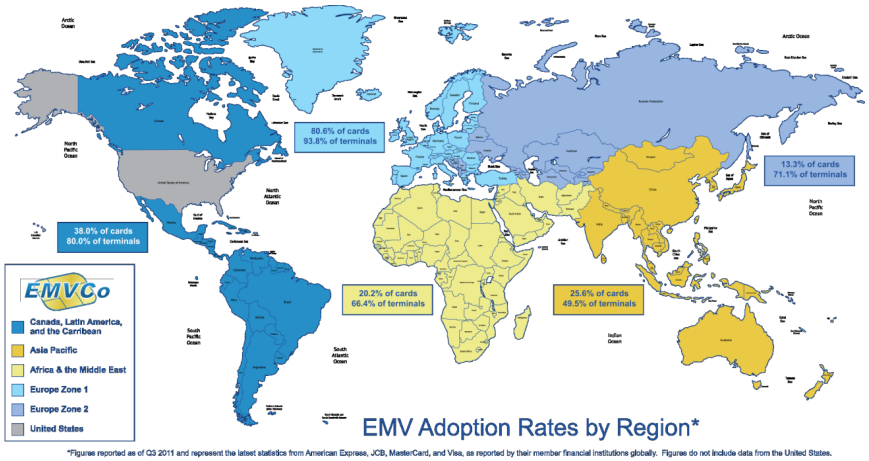

Figure 1: EMV adoption rates (source: EMV Adoption rates 2011, 2011)

A magnetic stripe can be more easily duplicated and exploited than a chip (Chu, Cheng, & Cheng, 1995; Berghel, 2007; Lamberger, 2009). Criminals did, however, because of the EMV standard, change their *modus operandi* and there is now a situation which could, from the criminological aspect, be called a type of crime displacement. Criminals have shifted from those types of abuses of payment cards, where there is a need for physical access to the card (like skimming), to the types where they only need the data from the payment cards. These data can be obtained through computer breaches of the data systems of card issuers, breaches in restaurants or stores, also home computers, or by social engineering, or even with data collected form our trash, and so on. These are called "card-not-present schemes" (Wiese & Omlin, 2009; Prabowo, 2011). Occurrences of classic types of abuses such as skimming are still prevalent, due to the duality of data holders on the payment card; the chip technology is not globally in use and the magnetic stripe is still present on the payment card. This is a situation where we have "anti-burglary doors, but leave the windows open". Criminals copy data from the magnetic stripe and then use the data to make fake cards and exploit them in regions where chip technology is not yet implemented.

Basic characteristics of abuses (Združenje bank Slovenije, 2002: 30):

- Well organized (card) crime specialized for certain areas.
- Links between the underworld and the (re)sources in financial institutions.
- Links between the underworld and fraudulent traders.
- Knowledge of technological features and security mechanisms.
- Easily accessible technology (magnetic readers, technical specifications on the Internet, phantom POS terminals);
- Cards weaknesses.
- Unlimited possibilities for testing.
- Different sources of information on the cards.
- Bank statements and information about payment card traffic are received only once a month.

Table 1 presents numbers of Slovenian police investigations of payment card related crimes since 2001.

Article[2]	2001	2002	2003	2004	2005	2006	**2007**	**2008**	**2009**	**2010**
253	1.865	2.516	2.687	1.465	2.158	2.625	2.110	1.496	774	428
247	0	0	0	0	0	0	0	3	424	1.075

Source: Letna poročila o delu policije [Annual reports on the work of the police] (n. d.)

Table 1: Number of investigated cases regarding payment cards

As seen in Table 1, there is reason to believe that after the introduction of article 247 of the penal code, these criminal acts were more often classified as such. The new article probably describes the acts more in tune with modern technology. The police did not give any other official reasons for this shift in numbers.

When academically dealing with payment card related crimes, several problems can arise. First, there is a lack of data from banks and other card issuers, primarily because banks are cautious and are afraid of getting a bad reputation (Lamberger, 2011). On the other hand, payment cards are *per se,* the only area in which banks are seek cooperation, at least in Slovenia. Here a special dialog was established between the police and the banks regarding information about the status of specific credit cards; if they are reported lost, stolen or missing. But no other data is revealed. Secondly, there is not a lot of expert literature in this area. This is good because criminals find it difficult to learn new things and become better at these activities. But it is a problem for criminalists if good investigation practices and preventive measures are not globally known. Contrary to this is the situation in the area of technology and payment cards, where there are almost daily improvements or new developments, which are often published in academic journals. Yet technology can only bring extremely limited results if it is not accompanied by broader social, criminological and daily analyses of practical cases.

2 INVESTIGATION OF PAYMENT CARD RELATED CRIMES

There are several subtypes of payment card crimes. Koppenhaver (2007: 181) for instance, lists the following six types: (1) Use of lost cards by unauthorized individuals; (2) Use of stolen cards by unauthorized individuals; (3) Altering a credit card; (4) Counterfeiting credit cards; (5) Fraudulent applications for credit cards; and (6) Fraudulent use of someone's credit card number. Other scholars have similarly categorized them into: Lost or stolen card, cash machine fraud, skimming/card copying, card-not-present fraud, foreign fraud, and identity (ID) theft (MONETOS, 2012). There was also a trend in card-not-received frauds or instances when criminals intercepted cards, often by attacking postmen, since it is

2 *Article 253 of – Presentation of Bad Cheques and Abuse of Bank or Credit Cards (); Article 247 of Penal Code of RS – Using a Fake Bank, Credit or Other Cards (Kazenski zakonik RS, 2008). Article 247 is only in power since November 1st, 2008.*

known that postal services also deliver payment cards (Lewis in Maniam & Earl, 2006).

We have grouped fraud and abuse in this area into four major groups:[3]

- Abuse or misuse by the rightful owner of the payment card.
- Abuse of lost or stolen payment cards.
- Frauds regarding counterfeit cards.
- Abuses and frauds connected to identity theft.

It should be emphasized that regardless of the subtype of payment card fraud or abuse, there are some distinctive criminal investigation commonalities. The first pertains to legislation. If the law does not keep up with new forms of criminal behavior, certain acts don't qualify as illegal nor can they be penalized, and therefore not even properly investigated.[4] The Second is related to the establishment of an effective information system which is active in real-time. The above mentioned PCI standard is a part of this, but it is not sufficient in its stand-alone form. It should be complemented by so-called "neural technology" that monitors and detects anomalies in payment card traffic (Aleskerov, Fieisleben, & Rao, 1997; Wiese & Omlin, 2009). This includes the detection of simultaneous payments at different locations, payments made in foreign country, etc. (Ghosh & Reily, 1994).

2.1 Investigation of Abuse or Misuse by the Rightful Owner of the Payment Card

In the instance when the rightful owner of the payment card is in so much debt that he is unable to pay the monthly bills for his credit card,[5] the role of repressive organs can sometimes be disputable. Even though there are cases of people who really have no intention of repaying their debts (Ghosh & Reily, 1994),[6] and such acts are always done with intent (Lamberger, 2011), there can be additional problems of proving the motive and intent in these cases. This is because accumulated debt is the result of bad financial decisions and a lack of self-control. A review of the literature and analyses of some financial situations have shown us that

3 *It seems that there are also constant re-occurrences of some old frauds in updated versions, only adjusted to new technologies and new designs of ATMs. The re-occurrences of "cash trapping", for instance – perpetrators obstruct the ATM's function of paying out the money. The transaction is completed and an amount is deducted from the victim's account, but the bills get "stuck". Victims believe that the transaction was correctly terminated, but after they step away from the ATM, perpetrators release the cash slot and take the "stuck" bills. Such types of crimes, with similar variations (like theft at ATM points), could be a fifth category – acts at point of service.*

4 *In Slovenia, relevant legislation is in power from November 1st, 2008. On that date a new criminal code came into effect, whereas acts of usage of counterfeited cards and similar abuses of payment cards can now be penalized. Before that, such crimes were treated as a form of grand larceny (Lamberger, 2011).*

5 *Only credit cards and cards with delayed payment options can be misused and exploited in fraudulent schemes.*

6 *The Slovenian legislation has (article 253 of the Slovenian Penal code) criminalized acts when a person (or persons) uses a credit card fully knowing that they will not be able to repay the amount spent (Kazenski zakonik RS, 2008).*

some countries have serious problems because a large number of residents are in extreme debts due to improper credit or similar card usage. Especially problematic is the situation in the USA (Fightmaster, 2009), and similar problems are reported in New Zealand (Lie, Hunt, Peters, Veliu, & Harper, 2010), Great Britain (Richards, Palmer, & Bogdanova, 2008), and elsewhere. In extreme situations, banks and card issuers reclaim the abused cards and legally seize the owner's property in order to repay their accumulated debt. In such cases the courts (especially civil courts) play a certain role, meanwhile the role of the police and criminal investigators is limited to providing safety for the for the entity who seizes the property. Only if the act was intentional are the police obligated to find the person, which is not too difficult, because the bank has all the necessary information about the credit card holder (Lamberger, 2011).

Some claim that currently when almost immediate authentication of a person's financial state is possible (due to chip technology and fast communication networks), such spending behavior can no longer go unchecked. But in fact chip technology hasn't been globally adopted, and due to non-centric bank systems a person can have multiple accounts and his shopping sprees go unnoticed.[7] Furthermore, not all big debts are the result of intentional or planned spending or lack of financial self-control. Debt can also be accumulated because of sudden unexpected reasons (Gradišar & Lamberger, 2010). In these cases, the subject's motive and intend are also important. These two aspects of criminality can also easily be seen (even if they are a bit more difficult to prove) in cases where overspending was done with a stolen, lost or counterfeit card.

2.2 Abuse of Lost or Stolen Payment Cards

There are four basic ways criminals can get hold of a payment card. They can steal it from the rightful owner; the card is one of the primary targets.[8] Secondly they can steal it, but theft of the card wasn't necessary the primary goal; this happens during burglaries, robberies and various forms of thefts where the payment cards are just "collateral damage" (Zupančič, 1999). The third includes attacks on couriers or postmen, while they are delivering payment cards to their owners (Lewis in Maniam & Earl, 2006). Such occurrences and frauds are usually named or categorized as card-not-received frauds, due to improved delivery methods these types of frauds are decreasing. Finally, a perpetrator gets a payment card if the owner loses it.

The crucial thing here is the speed of reporting the missing payment card. Perpetrators are aware of the fact that the card cannot be totally blocked for the first 24 hours from the time it was reported missing, so in 90% of the cases they exploit

7 *There are also some innuendos that banks permit such behavior as they profit from the resulting negative interest (especially in the USA) (McGeehan, 2004; Rummel & Kheyfets, 2004).*

8 *Here we could say that the so-called Lebanese loop is a type of fraud used to directly acquire a payment card. The Lebanese loop is similar to "cash trapping", the only difference is that here the payment card is trapped, taken and abused. The most advanced version is the placement of fake ATMs, where cards are skimmed, and PIN numbers are recorded.*

the illegally gained card within this timeframe (Lamberger, 2011). Here merchants are sometimes to blame because they rarely check the authenticity of a customers ID or if the signature on the card is a match (Downing Jr. & Geller, 2009). After the PIN number was introduced, even less attention was given to checking to see if the carrier of the card is the rightful owner (as long as the PIN is entered correctly, but the number can also be stolen). In most cases, cards are used for paying small fees (amounts under so-called floor limits) so that perpetrators don't attract too much attention. Higher amounts are spent only when the card is used immediately after illegal acquisition. If the amount is very high merchants are required to get additional authorization (Abanka Vipa, 1999: 2), and merchants are liable for damages in instances of unauthorized high-value purchases. Sometime the act is done in collaboration between merchant and perpetrator.

Investigation is extremely difficult and varies slightly in regard to the manner in which the card was obtained. If the card was lost it's a big setback because it is very hard to pinpoint the place of loss and narrow down possible suspects. In the case of a burglary more data is available, especially if the *modus operandi* of the perpetrator is known to the investigators. Pawnshops, online auction shops and personal ads are also used for selling the loot (the payment card is seldom the only target). After a robbery we have a personal description (at least of the perpetrator's height and shape or clothes). In other forms of thefts (for instance pick-pocketing) where payment cards were also stolen information on the location and *modus operandi* can also be derived.

2.3 Frauds Regarding Counterfeit Cards

The main problem of investigating counterfeit cards is discovering the point where the original card was copied. This is even more true currently because counterfeit cards can be produced in a variety of ways. They can be produced with data that were acquired by skimming or with data collected by penetrating the information system in which card information was stored (Maniam & Earl, 2006; Montague, 2011; Albrecht, Albrecht, & Tzafrir, 2011), e.g. card issuers' databases, shopping malls, and restaurants (Liebowitz, 2011). As previously mentioned, the introduction of chip technology has had some effect on these types of abuses, but unfortunately in more of an adaptive sense, as the perpetrators have changed their *modus operandi* and are still skimming payment cards worldwide. However, counterfeit payment cards are now only useable in regions, where chip technology has not yet been completely adopted. The current *modus operandi* has exceptional similarities to organized and/or transnational crime (EUROPOL Review, 2011; EUROPOL, 2011). Two of these are distinctive for the EU. A small group enters one of the EU countries, often in the tourist season, (Lamberger, 2011), sets skimming devices (either on ATMs or POS terminals) leaves them there for a period of time, accumulates data and then either sends it to a partner in a foreign country or (now more rarely) immediately uses the data to get some financial value. After they get their hands on the money, however, it is instantly transferred to third parties so there is no connection to the perpetrator (in case of an arrest), and so money

is quickly laundered. In the first case, the data transferred out of the country is then used to make a counterfeit card that can be exploited in regions without chip technology.

Slovenian investigators have noticed two similarly distinctive *modus operandi* in crimes related to payment cards. Perpetrators from Romania, Bulgaria, Croatia and Hungary come in groups of three, with large quantities of counterfeit cards which are then used to acquire money or goods. Those are then instantly transformed into currency, and the money is quickly transferred abroad through Western Union or similar wiring services. There were incidences when the stolen money was used to buy prepaid telephone cards which were then used to call specific numbers in foreign countries (payable telephone services) and financial benefit was provided to the owners of certain telephone numbersthus blurring the trace and laundering the money. After two to five days, the criminal groups leave the country (Lamberger, 2011). We have reasons to believe that this kind of activity will decrease.

A different kind of crime includes skimming payment cards and transferring the so collected data to other cards with magnetic stripes which are then used in Romania and Bulgaria (ibid.).

The most important investigative elements are: speed (because of migrating perpetrators), a cautious pre-planed approach (in order not to alert and alarm the suspects who are usually in close proximity of the machine/system where the skimming device is attached, because of the limited power of the transmitters used), and cooperation (ibid.). Cooperation must be established within the country. Proper training should be provided for investigators, bank personnel or ATM caretakers (if they notice a skimming device on an ATM or if the machine had retained a counterfeit card these elements represent a crime scene and great care must be taken to properly examine and document it). Cross-border cooperation is also crucial, due to the highly migratory and organized/transnational crime characteristics of such criminal acts.

2.4 Abuses and Frauds Related to Identity Theft

The new prevailing types of crimes related to payment cards are crimes where only information from the payment card is stolen or abused. These so-called card-not-present schemes (Wiese & Omlin, 2009; Prabowo, 2011) are primarily a byproduct of the increasing numbers of subjects dealing with card data on a daily basis (from new stores to new consumers), and of the fact that new consumers lack computer skills and are incautious or not aware of the dangers and so represent easy targets for skilled computer crackers and hackers. Secondly, there are now more cases of card-not-present frauds due to the introduction of chip technology (ibid). Even though the frequency of these crimes has greatly increased only lately, the history of these frauds is long, dating back to times when payment cards were first introduced to consumers on a large scale. Previously, perpetrators had first used illegally acquired data from telephone payment cards, and later from cards for shopping on the Internet (Ghosh & Reily, 1994; Aleskerov et al., 1997; Berghel, 2007; Wiese & Omlin, 2009; Sullivan, 2010; Montague, 2011). Stolen personal

information (home address, social security number, bank information) could be abused to acquire specific financial gain (like credit) and the victims discovers that his identify was stolen only when they receive the bills to repay credit card debt or for purchased goods (Ghosh & Reily, 1994; Jackson, 1994).[9]

Investigative approaches are similar to those used in dealing with counterfeit cards. Following the way from the point where data was tapped, by using data on illegally acquired goods, they back-tracked to the perpetrators. Time is of the essence as the longer perpetrators stay undetected the more options they have to launder the money.

No matter which subtype of payment card crime (or for that matter any type of crime) is in play, repressive organs must be active from the moment that prevention fails. Their role is diverse. Probably the most common task ascribed to them is the apprehension of the criminal(s) and by doing so upholding general prevention. As is evident, crimes related to payment cards have characteristics of economic crimes, which means they are therefore often complex, covert, sort of "invisible" (Gradišar & Lamberger, 2010); and characteristics of organized (transnational) crime (Zupančič, 1999). Levi & Handley (2002) emphasize the additional investigative difficulties due to the fact that these crimes are carried out in cyberspace, that investigators lack certain knowledge, and the final obstacle being the question: Who will finance the investigation? Lamberger (2011) adds that further difficulties arise because bank data is classified.

The key element in dealing with almost any crime, especially economic ones, is the confiscation of illegally gained assets. This is crucial because confiscation makes crimes not worthy of the risk (part of general prevention) and because money is the evidence and could be used in trials (ibid).

3 CONCLUSIONS

It does seem that technological advances have resulted in some improved safety measures for our payment cards. But it also seems that payment cards are one area of society where globalization appears to be limited. Payment card usage is global, but the newest preventive technology is only slowly becoming unified all around the world, as exemplified by the not yet globally implemented EMV standard. As mentioned in the Introduction to this paper one of the elements of payment cards is still quite unsecure. The magnetic stripe (alongside the safer chip), represents the key weakness of payment cards, the magnetic stripe is misused in a majority of skimming incidences. In the future perpetrators will probably also find a way to crack the chip technology as well. For now they rely on the fact that we have "left a window open for them" even though we have currently the best "anti-burglary doors".

The impact of the EMV standard has resulted in a modification of the perpetrators' *modus operandi*. Now emerging and proliferating are new forms of

9 *As mentioned, personal data can be gathered from our trash, from papers that we carelessly throw away instead of been destroyed (Albrecht et al., 2011).*

card-not-present frauds. Some believe that these types of frauds are becoming the most dangerous (Prabowo, 2011). Statistical data confirms this belief, and major card issuers are already developing additional protocols (like 3D passwords) to achieve greater safety in on-line shopping. The second direct consequence of the implementation of the said standard is that perpetrators have become even more mobile. They travel to countries where the EMV standard is implemented, but they skim the ever-present magnetic stripe on cards and send the copied data to their counterparts in regions where chip technology has not yet been totally adopted. In the course of their illegal activities evidence gets lost and proving crimes becomes even harder.

Bank employees and criminal investigators are people who must daily combat clever perpetrators who use technology inventively. Bank employees do have access to the latest technology, global fast replying connections, and the best overview of such crimes, but much more is expected of criminal investigators, who have limited budgets, extensive workloads and limited data on crime. However, investigators do have good international cooperation, in which the roles of EUROPOL and INTERPOL are crucial and extremely beneficial (as seen from their annual reports). Cooperation, knowledge of technological advances, strategic and criminal investigation skills are elements that enable the police to carry out relatively successful investigations and promote prevention. They would however benefit from academic research of payment card crimes and could use more data from banks. Academic studies bring concise conclusions and information that criminal investigators do not have the time and the means to compile by themselves. Cooperation between card-issuing companies, repressive organs and academic institutions (such as the Faculty for Criminal Justice and Security) could perhaps bring new insight. Of course, data provided by banks should be the "pool of knowledge" from which flow new conclusions. Even rough bank data could be useful to investigators, and even more to the developers of preventive measures. The main problem or weak point in a system of preventive measures, are its developers. Programmers and information technology experts who daily develop new security programs, protocols and similar codes, don't know enough about criminal investigation. Their safety improvements are sometimes more reactive than pro-active. On the other hand investigators are limited because they don't always have computer expertise or knowledge of economics. And although preventive measures still seem to be the best possible action, they should be a result of multi-profession collaboration, nor just a product of a single field.

In the end, it can be said that the key problem could possibly be that we are dealing with to much data. We are being buried beneath data and finding relevant and important information is becoming more and more of a problem. This is as true for investigators and as for the average card user, who can only seldom know, that among the daily processed data there is a fragment produced by a criminal in order to trick them.

REFERENCES

Abanka Vipa. (1999). *Plačilne kartice*: *seminar* [Payment cards: Seminar]. Ljubljana

Albrecht, C., Albrecht, C., & Tzafrir, S. (2011). How to protect and minimize consumer risk to identity theft. *Journal of Financial Crime, 18*(4), 405-414.

Aleskerov, E., Fieisleben, B., & Rao, B. (1997). CARDWATCH: A neural network based database mining systern for credit card fraud detection. In *Proceedings of the IEEE/IAFE 1997 Computational Intelligence for Financial Engineering (CIFEr)* (pp. 220-226). Piscataway: IEEE.

Berghel, H. (2007). Credit card forensics: Decoding the magnetic attraction of criminals to swiping. *Digital Village, 50*(12), 11-14.

Chu, M., Cheng, L., & Cheng, L. (1995). A Novel magnetic card protection system. In *European Convention on Security and Detection, 16-78 May 799R Conference Publication No. 408* (pp. 207-211). Brighton.

Downing Jr., C. O., & Geller, E. (2009). Behavior analysts address credit-card fraud. *Behavior Analysis Digest International, 21*(4), 13-14.

EUROPOL review: General report on EURPOL activities for 2009. (2011). Retrieved from https://www.europol.europa.eu/sites/default/files/publications/europolreview2009.pdf

EUROPOL: Major international network of payment card fraudsters dismantled. (2011). Retrieved from https://www.europol.europa.eu/content/press/major-international-network-payment-card-fraudsters-dismantled-1001

Fightmaster, M. (2009). President Obama to meet with credit card execs. *DailyFinance.com*. Retrieved from: http://www.dailyfinance.com/story/president-obama-to-meet-with-credit-card-execs/1525783/

Ghosh, S., & Reily, D. L. (1994). Credit card fraud detection with a neural-network. In *System sciences. Vol. 3: Information systems: Decision support and knowledge-based systems, Proceedings of the Twenty-Seventh Hawaii International Conference* (pp. 621 - 630). Wailea.

Gradišar, M., & Lamberger, I. (2010). Vpliv represivnih dejavnikov na zlorabe kreditnih in plačilnih kartic v Sloveniji [The impact of repressive factors on abuse of credit and debit cards in Slovenia]. *Revija za kriminalistiko in kriminologijo, 61*(1), 28-36.

Jackson, J. E. (1994). Fraud masters: Professional credit card offenders and crime. *Criminal Justice Review, 19*(1), 24-55.

Kazenski zakonik RS [Penal Code of RS]. (2008). *Uradni list RS*, (55/08).

Koppenhaver, K. M. (2007). *Forensic document examination: Principles and practice.* New Jersey: Humana Press.

Lamberger, I. (2009). Vpliv represivnih organov in generalne prevencije na področju zlorab kreditnih in plačilnih kartic [The impact of repressive factors and general prevention in the field of payment cards]. In T. Pavšič Mrevlje (Ed.), *Zbornik povzetkov, 10. slovenski dnevi varstvoslovja.* Ljubljana: Fakulteta za varnostne vede.

Lamberger, I. (2011). *Model zaščite elektronskih plačilnih sistemov pred zlorabami* (Doktorska disertacija) [A model of electronic system protection against misuse (Dissertation)]. Ljubljana: Faculty of Economics.

Letna poročila o delu policije [Annual reports on the work of the police]. (n. d.). Retrieved from http://www.policija.si/index.php/statistika/letna-poroila

Levi, M., & Handley, J. (2002). *Criminal justice and the future of payment card fraud*. London: IPPR Criminal Justice Forum.

Lie, C., Hunt, M., Peters, H. L., Veliu, B., & Harper, D. (2010). The "negative" credit card effect: Credit cards as spending-limiting stimuli in New Zealand. *The Psychological Record, 60*(3), 399-411.

Liebowitz, M. (2011). *Romanian hackers charged in subway sandwich card-swipe scheme*. Retrieved from http://www.securitynewsdaily.com/romanian-hackers-subway-sandwich-scheme-1409/

Maniam, B., & Earl, R. (2006). Perspectives on credit card use and abuse. *Journal of American Society of Business and Behavioral Sciences, 2*(1). Retrieved from http://www.asbbs.org/files/2006/ASBBS%20E-Journal%202006%20HTM%20Files/perpectives%20on%20credit%20asbbs%20e-journal%202006.pdf

McGeehan, P. (2004). Soaring interest compounds credit card pain for millions. *The New York Times*. Retrieved from http://www.nytimes.com/2004/11/21/business/21cards-web.html?_r=1&hp&ex=1101099600&en=70effacd11d42b21&ei=5094&partner=homepage

MONETOS. (2012). *Types of credit card fraud*. Retrieved from http://www.monetos.co.uk/financing/credit-cards/fraud-protection/types/

Montague, D. (2011). *Essentials of online payment security and fraud prevention.* New Jersey: John Wiley & Sons.

PCI Security Standards Council. (2011). *About us.* Retrieved from https://www.pcisecuritystandards.org/organization_info

Pcistandard.com. (2011). Retrieved from http://www.pcistandard.com/pci_standard.html

Prabowo, Y. H. (2011). Building our defense against credit card fraud: A strategic view. *Journal of Money Laundering Control, 14*(4), 371-386.

Richards, M., Palmer, P., & Bogdanova, M. (2008). Irresponsible lending? A case study of a U.K. credit industry reform initiative. *Journal of Business Ethics, 81*(3), 499–512.

Rummel, D., & Kheyfets, K. (2004). *Frontline: Secret history of the credit card* (Documentary film). Public Broadcasting Service. Retrieved from http://www.pbs.org/wgbh/pages/frontline/shows/credit/v

Sullivan, R. J. (2010). *The changing nature of U.S. card payment fraud: Industry and public policy options.* Kansas City: Federal Reserve Bank. Retrieved from http://www.kansascityfed.org/Publicat/Econrev/pdf/10q2Sullivan.pdf

Wiese, B., & Omlin, C. (2009). Credit card transactions, fraud detection, and machine learning: Modelling time with LSTM recurrent neural networks. In M. A. Bianchini, M. Maggini, F. Scarselli, & L. C. Jain (Eds.), *Innovations in neural information paradigms and applications* (pp. 231-268). Berlin: Springer.

Združenje bank Slovenije. (2002). *Ponaredki in druga kriminalna dejanja pri kartičnem poslovanju* [Counterfeits and other crimes in cards related businesses], *seminar, Tacen 6. 3. 2002*. Police academy.

Zupančič, M. (1999). Zlorabe plačilnih kartic pri elektronskem poslovanju [Abuse of payment cards in electronic commerce]. *Revija za kriminalistiko in kriminologijo*, *50*(3), 215-224.

About the Authors:

Igor Lamberger, PhD, employed at the General Police Directorate, lecturer at the Slovenian Police Academy and senior lecturer at the Faculty of Criminal Justice and Security, University of Maribor; igor.lamberger@policija.si

Bojan Dobovšek, PhD, associate professor and vice-dean of the Faculty of Criminal Justice and Security, University of Maribor, Slovenia; bojan.dobovsek@fvv.uni-mb.si

Boštjan Slak, postgraduate student at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia.